

SALOWEY
Appl. No. 09/524,272
July 12, 2004

REMARKS/ARGUMENTS

Applicant respectfully requests the Examiner to reconsider and allow this application in view of the claim amendments and the following remarks.

Applicant has amended each independent claim herein to more particular point out the invention. Each claim now requires, in combination and among other things:

- a "client web browser and virtual machine being of the type that download and execute applets while protecting at least some of said client resources from being affected by said applet execution" (or similar);
- "downloading, over an insecure network, said at least one applet including:
(a) a second key corresponding to the server, (b) code executable on the client virtual machine to cause the client to store the second key, and (c) code executable on the client virtual machine to establish a secure network connection with said server"; and
- establishing a secure network connection under control of the executing applet.

These features in combination are not taught or suggested by the applied prior art.

The Examiner appears to concede that Sudia does not teach a web browser, a virtual machine or executing applets, but he contends that it would have been "obvious" to modify Sudia along the lines of Draper. However, Draper does not teach or suggest the features quoted above. For example, Draper's distributed database does not address

SALOWEY
Appl. No. 09/524,272
July 12, 2004

the same problem as applicant has solved (i.e., how to establish a secure network connection between a web browser and a server when the web browser has no means to authenticate the server).

The newly cited Curtis patents similarly do not teach or suggest the claimed subject matter. For example, Curtis relies on a secure connection for delivering a key used to authenticate the server certificate. See e.g. Curtis '544 at col. 7, line 3 ("a secured connection is established ...") Compare with applicant's specification at page 7 lines 21 and following ("Another option might be to require the applet and certificate to be transmitted over a secure (e.g., SSL) session between the platform 54 and the service 60. This would work, but is undesirable because such secure sessions increase the amount of loading and overhead on the service 60 for each connection")

Finally, as discussed during the 22 June 2004 Interview, while applicant respectfully disagrees with the Examiner's interpretation of the term "secure connection" as being, in the context of applicant's specification, anything other than a "secure network connection", applicant has amended his claims to make explicit what he believed was already there. In addition, during the interview, the Examiners specifically asked about Sudia's disclosure at col. 28, line 36 and following. However, that part of Sudia does not appear to teach establishing a secure network connection using an applet executing within a web browser in combination as claimed herein.

All outstanding issues have been addressed and this application is in condition for allowance. Should any minor issues remain outstanding, the Examiner should contact the


BEST AVAILABLE COPY

SALOWBY
Appl. No. 09/524,272
July 12, 2004

undersigned at the telephone number listed below so they can be resolved expeditiously
without need of a further written action.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

Robert W. Faris
Reg. No. 31,352

RWF:ej
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

BEST AVAILABLE COPY